

UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

2309 Cockrells Run Rd., Lucasville, OH 45648

Case No. **1:23-MJ-00048**

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252(a)(2)&(a)(4) (4); 18 U.S.C. §§ 2252A(a)(2) (A) & (a)(5)(B)	Receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct/Possession of and access with intent to view

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

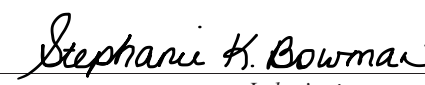
Ryan Sutphin, Special Agent HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
FaceTime Video Conference (specify reliable electronic means).

Date: Jan 23, 2023

City and state: Cincinnati, Ohio

  
Judge's signature

Stephanie K. Bowman, United States Magistrate Judge

Printed name and title



**ATTACHMENT A**

*Property to be searched*

The property to be searched is 2309 Cockrells Run Rd., Lucasville, OH 45648 (the SUBJECT PREMISES). The SUBJECT PREMISES is a single-story ranch house with a brick exterior and detached two car garage connected to the SUBJECT PREMISES with a shared roof. There are three visible windows on the front of the SUBJECT PREMISES visible from the street and a south/southwest facing entry way on the front porch.

The SUBJECT PREMISES to be searched includes the persons of Ashley Boyer and Seth Boyer, if they are present at the SUBJECT PREMISES, or return to the SUBJECT PREMISES, at any point during the execution of the search warrant.





**ATTACHMENT B**

*Property to be seized*

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the “Target Offenses”), those violations involving an unidentified suspect including:

- a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256.
- b. Child erotica.
- c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
- d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography, whether transmitted or received.
- e. Records and information concerning Kik or Meetme.

- f. Records, information, and communications concerning or discussing a sexual interest in Minors.
- g. Records and information relating to the ownership or possession of the PREMISES.
- h. Records and information relating to the email account [davebounts15@gmail.com](mailto:davebounts15@gmail.com), Kik account davebounts, and any other accounts used in furtherance of the Target Offenses.
- i. Records and information relating to online applications and cloud-storage applications that could be used to commit the Target Offenses, including usernames and passwords for those applications.
- j. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.



- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. evidence of the lack of such malicious software.
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation.
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence.
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.
- h. evidence of the times the COMPUTER was used.
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER.

- k. records of or information about Internet Protocol addresses used by the  
COMPUTER.
  - l. records of or information about the COMPUTER's Internet activity, including  
firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"  
web pages, search terms that the user entered into any Internet search engine, and  
records of user-typed web addresses.
  - m. contextual information necessary to understand the evidence described in this  
attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
THE RESIDENCE LOCATED AT:

2309 Cockrells Run Rd., Lucasville, OH  
45648

Case No. 1:23-MJ-00048

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Sutphin, a Special Agent with Homeland Security Investigations, being duly sworn,  
depose and state as follows:

**INTRODUCTION**

1. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2309 Cockrells Run Rd., Lucasville, OH 45648 (the “**SUBJECT PREMISES**”), further described in Attachment A, and the person of Ashley Nicole BOYER (date of birth: January 2, 1989) and Seth Edward BOYER (date of birth: March 16, 1983), provided that these persons are located at the **SUBJECT PREMISES** and/or within the Southern District of Ohio at the time of the search, for the things described in Attachment B.

2. I have been employed as a Special Agent (SA) of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since March 2020. During my tenure as a Federal Law Enforcement Officer, I have completed the Uniform Police Training Program (UPTP), Criminal Investigator Training Program (CITP), and the Homeland Security Investigations Special Agent Training Program (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I have received training on cybercrimes, child exploitation, child pornography, and the dark web and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C.

§ 2256) in multiple forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The statements in this Affidavit are based on information provided by other law enforcement officers and on my investigation of this matter. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts in this Affidavit, I submit that there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a prepubescent minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography involving a prepubescent minor) are presently located at the **SUBJECT PREMISES**.

**PERTINENT FEDERAL CRIMINAL STATUTES**

5. This investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1), prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or

foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2), prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1), prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Pursuant to Title 18, United States Code, Section 2256, the term sexually explicit conduct includes the lascivious exhibition of the genitals or pubic area of any person.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET**

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four (4) functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as digital files that can be directly transferred to another device using a cable or via wireless connections such as “WiFi” or “Bluetooth.” In the last ten (10) years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning

that such pictures have become sharper and crisper. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Printed photographs can also be transferred to a digital format with a device known as a scanner.

c. A device known as a modem allows a computer to connect to another computer through a telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte or larger external and internal hard drives are not uncommon. It is extremely easy

for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Some media storage devices can easily be concealed and carried on an individual’s person or in an individual’s vehicle. Smartphones and/or mobile phones are often carried on an individual’s person. Additionally, devices and other electronic storage media can be found in an individual’s vehicle.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or

unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE,  
DISTRIBUTE, AND/OR POSSESS CHILD PORNOGRAPHY**

7. As a result of my training and experience in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt, distribution, and possession of child pornography.

a. These individuals may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasizing while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. These individuals may collect sexually explicit or suggestive materials, in a variety of media, including digital and electronic media, photographs, magazines, motion pictures, video tapes, books, sliders, drawings, and/or other visual media. These individuals often use these materials for their own sexual arousal and gratification. Furthermore, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.



c. To the extent these individuals possess and maintain “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., they almost always maintain those hard copies in the privacy and security of their home. They typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. Likewise, these individuals often maintain their digital or electronic collections of child sexual exploitation images in a safe, secure, and private environment, such as a computer and surrounding area, or on cellular telephones. These collections are often maintained for several years and are kept close by, usually at the individual’s residence, on his or her person, or in his or her vehicles, to enable the individual to view the collection, which is valued highly. It is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices to obtain, store, or share their collections. Increasingly, individuals who view child pornography are utilizing laptop computers and other smaller devices, such as cellular telephones, iPads, and tablets to do their computing.

e. These individuals also may correspond with and/or meet others to share information and materials; are rarely able to destroy correspondence from other child pornography distributors/collectors; conceal correspondence related to their sexually

explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. These individuals prefer not to be without their child sexual exploitation images for any prolonged time period. Collectors will take their collection with them if they change residences, as the collection is considered to be a prized possession. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. That said, there are individuals with a sexual interest in children who download and view digital images of child sexual exploitation and delete them in order to avoid detection by law enforcement or other people. However, even in cases where these images are deleted, or concealed via encryption software, forensic examiners can sometimes use specialized tools to recover the deleted files or access encrypted files.

g. These individuals often use specialized software to conceal the existence of evidence and/or destroy said evidence. There are a variety of different programs that an individual can use to accomplish these objectives, many of which are free. Additionally, these individuals have been known to store child pornography in unconventional physical locations, as well as in unusual digital locations on computers and cellular phones. These files and folders, or applications, have been misnamed or renamed in an attempt to mislead investigators.

h. These individuals will often download and store images of children they know or with whom they have communicated, as well as their communications with those

children. The images may not necessarily be pornographic or obscene in nature; however, they are often used for the individuals' sexual gratification.

### **BACKGROUND OF CHAT APPLICATION**

8. This investigation involves Kik, a secure chat platform. Kik is a communications platform based in the United States. Service is offered through a mobile application for iOS and Android operating systems. Kik's service includes instant messaging and file sharing capabilities. To create and subsequently log into Kik, a user must provide an email address for verification, a username, and a unique password. Communication on Kik is end-to-end encrypted and stored locally on the device used, meaning only the user can decrypt content stored on the device that is accessing Kik. Communication on Kik is ephemeral and offers multiple methods for automatically clearing chat history including a stored message limit, logging out of the account, or logging into the account from a different device.

9. Based on my training and experience and from information relayed to me by other law enforcement officers, I know Kik is often used for illegal activity including exchanging and accessing child pornography, because of the high degree of anonymity that Kik offers its users.

### **PROBABLE CAUSE**

10. On or about November 17, 2020, the United Kingdom (UK) National Crime Agency (NCA) coordinated with United States (US) law enforcement officials to safeguard a 13-year-old female who had reported online abuse by a UK citizen, known as username

“Trevor”. The NCA later identified the suspect as Trevor Fernandes (FERNANDES). The investigation revealed that FERNANDES coerced and forced the minor US female to engage in sexual activity with a dog and a 1-year-old child. Furthermore, FERNANDES maintained a Kik account that was used to exchange Child Sexual Abuse Material (CSAM), under the username “cuteandstrict”.

11. US law enforcement conducted a search warrant of the Kik account cuteandstrict. The return provided records of the chat messages and images that were sent and received by username cuteandstrict via Kik. The actual content was unavailable due to records retention policies. A review of these messages identified multiple accounts involved in the exchange of CSAM. One such account was username “davebounts”.

12. A subpoena was issued for subscriber information regarding Kik username davebounts. The return identified the following account information:

First name: Dave

Last name: BOUNTS

Email: DaveBounts15@gmail.com

Birthday: 03/16/1985

13. Furthermore, the results revealed that username davebounts sent cuteandstrict three images (9a9ee43c-4a8a-42f9-a2ea-70bf94a2188b, d87872f0-0cc4-4075-b762-993d5db36f8e and 5cb7c8ad-935b-4ee3-90b1-3f56ef1201b0) via Kik on October 14, 2020. The group username was titled “#11to14onlynopervsplease” and screenname “10 to 15 teen girls only ( need to verify )”. The NCA searched FERNANDES’s seized devices for the images and identified two:

- 9a9ee43c-4a8a-42f9-a2ea-70bf94a2188b displayed one (1) female child aged approximately 12 years old lying on a sofa on her back naked. She has her legs spread and is spreading open her vagina with her hands.
- d87872f0-0cc4-4075-b762-993d5db36f8e displayed two (2) female children aged approximately 12 years old lying on their backs naked. They have their legs spread and are touching their vaginas with their hands.

14. Law enforcement officials completed deconfliction of username davebounts and email davebounts15@gmail.com with the National Center for Missing and Endangered Children (NCMEC). NCMEC deconfliction revealed that the Kik username davebounts and suspect email address davebounts15@gmail.com is linked to a previous Kik cybertip (CT), 84247140, associated with the upload of 20 apparent CSAM files. Below is a summary of some files distributed using the Kik account davebounts between December 27, 2020, and January 4, 2021:

- One (1) video was approximately 0:15 seconds in length. The video depicted a fully nude prepubescent female, with little to no breast development and dental braces. The minor is lying down and the camera moves from her face to place her vagina as the focus of the video. The minor female then begins to spread open her vagina with her hand.
- One (1) image of a fully nude prepubescent female, with no breast development spreading her legs apart and leaning back. The minor female's vagina is fully exposed.

- One (1) video approximately 1:00 minute in length. The video depicted a prepubescent female with a garment made of denim like fabric around her waist and her vagina exposed to the camera. An adult male is shown forcing his erect penis into the body of the prepubescent female. Comparison of the adult male's penis and hand size in relation to the female's body size and lack of body hair indicates a minor female.

15. A review of CT 84247140 revealed multiple Internet Protocol (IP) addresses used to upload CSAM using the davebounts Kik account. A search of open-source information revealed one such IP address, 76.177.98.209, accessed on December 27, 2020, at 06:53:51 UTC is leased by Charter Communications, Inc. Records from Charter showed the IP address resolved to subscriber name: Ashley Boyer and service address: 133 Slocum Heights Rd., Portsmouth, OH 45662. The records showed that the lease for the account started on 09/08/2020 and ended on 12/31/2020.

**SUBSCRIBER RECORD**

<b>Target Details</b>	<b>76.177.98.209, 12/27/2020 6:53:00 AM, GMT, 0</b>
Subscriber Name:	ASHLEY BOYER
Service Address:	133 SLOCUM HEIGHTS RD, PORTSMOUTH, OH 456628643
Billing Address:	
User Name or Features:	7403576472@CHARTER.NET
Phone number:	7403576472
<b>Advanced Subscriber Info</b>	
Account Number:	8362210960005163
MAC:	945330E8C860
Lease Log:	Start Date: 09/28/2020 11:30 PM End Date: 12/31/2020 06:36 PM
<b>Equipment Details</b>	
CM MAC:	945330E8C85F
<b>Other Details</b>	
Other Information:	N/A

16. NCMEC deconfliction identified a second CT, 42888350, associated with the name “Seth Boyer”. A review of CT 42888350 revealed the Dropbox username “Seth Boyer” was associated with the upload of 42 apparent CSAM files between May 13, 2018, and September 7, 2018. IP addresses indicated multiple internet providers were used across multiple states indicating the suspect was traveling during the time frame. Internet provider records had exceeded record retention policies and were unavailable to identify the subscriber.

17. On or about June 8, 2022, investigators conducted a commercial law enforcement database search for Ashley Boyer revealing a current listed address at the **SUBJECT PREMISES**. This same search also corroborated a previous residential



address at 133 Slocum Heights Rd. in Portsmouth, Ohio. Commercial law enforcement database queries revealed approximately two individuals presently associated with the **SUBJECT PREMISES**. Specifically, the **SUBJECT PREMISES** was listed as a current address for Ashley Boyer, as well as Seth Boyer.

18. Scioto County marriage records show a marriage license was filed for Seth Boyer, DOB 03/16/1983, and Ashley Evans (Boyer), DOB 01/02/1989, on September 12, 2017, and records further indicated a marriage was officiated on September 16, 2017. A commercial law enforcement database check indicated Seth Boyer resided with Ashley Boyer at 133 Slocum Heights Rd., Portsmouth, OH 45662 beginning approximately March 2017.

19. On or about June 9, 2022, Ohio Law Enforcement Gateway (OHLEG) queries for the individuals referenced in Paragraph 17 revealed valid Ohio driver's licenses for both. Both individuals had the **SUBJECT PREMISES** listed as a current residence. Ohio Bureau of Motor Vehicles records checks identified that there were three vehicles registered with Seth Boyer's name at the **SUBJECT PREMISES**, a gold Ford F-150 bearing Ohio license plate GPY9216, a red trailer bearing Ohio license plate SZU5764, and a blue Hyundai Sonata bearing Ohio license plate HQU3320

20. On or about January 12, 2023, investigators conducted surveillance of the **SUBJECT PREMESIS**. Investigators observed the gold Ford F-150, bearing license plate GPY9216, and blue Hyundai Sonata, bearing license plate HQU3320, both parked in the driveway at the **SUBJECT PREMESIS**.

21. That same day investigators identified a wireless internet signal emitted from the **SUBJECT PREMESIS**. Investigators determined the wireless internet signal was provided through a subscription service to Frontier Communications Corporation.

22. On or about January 17, 2023, an administrative subpoena/summons was served upon Frontier Communications Corporation, for subscriber information and Internet Protocol (IP) addressees pertaining to the **SUBJECT PREMESIS**. That same day Frontier responded to the administrative subpoena/summons with the requested information and identified Ashley Boyer as the responsible party with a lease start date on January 12, 2021. Frontier records additionally provided an IP address history between the dates of January 14, 2021, through January 4, 2023. The most recent IP address assigned to the **SUBJECT PREMESIS** was 74.38.59.23 from July 5, 2022 through January 4, 2023.

23. NCMEC deconfliction of the above IP address identified a third CT, 135263196. A review of CT 135263196 revealed the MeetMe profile name “Seth”, identified with date of birth March 16, 1985<sup>1</sup>, and using email “sethboyer4568@gmail.com” was engaged in suspected online enticement of a minor for sexual acts on or about September 13, 2022. MeetMe profile “Seth” attempted to contact a female profile identified as a thirty-three-year-old female at approximately 02:08:31 eastern time. At approximately 02:11:23 the female account revealed to “Seth” she was 13 years old and attempted to end the conversation. “Seth” responded by saying “I’m fine with that if you are looking for a older man”. The minor female then stated “My mom

---

<sup>1</sup> In my training and experience, individuals conceal their age and identity by alternating names and birth dates on their online profiles.

would kill me”....”Now she gonna see this”. “Seth” continued the conversation guiding the minor female how to delete the chat so her mother would not see it and coerced the minor female to provide her phone number for an offline conversation. The online conversation concluded with the minor female confirming “Seth” copied her phone number and saying “Ok I’m going to delete now k” at approximately 02:22:16 eastern time.

24. Based on the evidence that the Kik user account, davebounts, was accessed using an IP address leased to Ashley Boyer at the residential address of 133 Slocum Heights Rd., during the identified time period the davebounts user account was engaged in the exchange of CSAM on Kik, and the two known individuals living at 133 Slocum Heights Rd. now both reside at the **SUBJECT PREMISES** and the conversation on MeetMe occurred from an IP address associated with the **SUBJECT PREMISES**, I believe that the user of the davebounts account now resides at the **SUBJECT PREMISES**.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

25. As described above and in Attachment B, this application seeks permission to search for certain records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause.* Given the information set forth above, I submit that if a computer or electronic storage medium is found on the **SUBJECT PREMISES**, there is

probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files and electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or electronic storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online usernames, nicknames, and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have

geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of



knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. *Necessity of seizing or copying entire computers or storage media.* Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes,

memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may

yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computers and electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

31. Because it appears that several people share the **SUBJECT PREMISES** as a residence, it is possible that the **SUBJECT PREMISES** will contain computers or electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or electronic storage media, the warrant applied for would permit the seizure and review of those items as well.

**SEARCH METHODOLOGY TO BE EMPLOYED**

32. All computers, other computer hardware, computer software, and any form of electronic storage media that could contain evidence described in this warrant may be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

33. The search procedure of electronic data contained in computers, other computer hardware, computer software, and/or electronic storage media may include the following techniques (the following is a non-exhaustive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices, or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software.

b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed.

c. Examination of all of the data contained in such computers, other computer hardware, computer software, or electronic storage media to view the data and determine whether that data falls within the items to be seized as set forth herein.

d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. Surveying various file directories and the individual files they contain.

f. Opening files in order to determine their contents.

g. Scanning storage areas.

h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

34. Contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

35. Because it is expected that the computers, other computer hardware, computer software, and any form of electronic storage media may constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be

returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

a. Because of the large storage capacity as well as the possibility of hidden data within the computers, other computer hardware, and any form of electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the computer, other computer hardware, or any form of electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

b. Further, because investigators cannot anticipate all potential defenses to the offenses in this Affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

c. If after careful inspection investigators determine that such computers, other computer hardware, computer software, and electronic storage media do not contain or constitute (1) instrumentalities of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

#### **BIOMETRIC ACCESS TO DEVICES**

36. This warrant permits law enforcement to compel Ashley Boyer and Seth Boyer to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.



c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes, and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are

considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days.

Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Ashley Boyer and/or Seth Boyer to the fingerprint scanner of the DEVICES found at the **SUBJECT PREMISES** or on the person of Ashley Boyer or Seth Boyer (2) hold the DEVICES found at the **SUBJECT PREMISES** or on the person of Ashley Boyer or Seth Boyer in front of the face of Ashley Boyer or Seth Boyer and activate the facial recognition feature; and/or (3) hold the DEVICES found at the **SUBJECT PREMISES** or on the person of Ashley Boyer or Seth Boyer in front of the face of Ashley Boyer or Seth Boyer and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Ashley Boyer or Seth Boyer state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Ashley Boyer or Seth Boyer to identify

the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

### **CONCLUSION**

37. Based on the foregoing, there is probable cause to believe that contraband, property, evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a prepubescent minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography involving a prepubescent minor), as described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

38. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the **SUBJECT PREMISES**. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



---

Ryan Sutphin  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me this 23rd day of January, 2023.  
**via electronic means, specifically Facetime video.**

*Stephanie K. Bowman*



---

HON. STEPHANIE K. BOWMAN  
United States Magistrate Judge  
U.S. District Court for the Southern District of Ohio

**ATTACHMENT A**

*Property to be searched*

The property to be searched is 2309 Cockrells Run Rd., Lucasville, OH 45648 (the SUBJECT PREMISES). The SUBJECT PREMISES is a single-story ranch house with a brick exterior and detached two car garage connected to the SUBJECT PREMISES with a shared roof. There are three visible windows on the front of the SUBJECT PREMISES visible from the street and a south/southwest facing entry way on the front porch.

The SUBJECT PREMISES to be searched includes the persons of Ashley Boyer and Seth Boyer, if they are present at the SUBJECT PREMISES, or return to the SUBJECT PREMISES, at any point during the execution of the search warrant.







**ATTACHMENT B**

*Property to be seized*

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4)(B), 2252A(a)(2), and 2252A(a)(5)(B) (the “Target Offenses”), those violations involving an unidentified suspect including:

- a. All visual depictions of child pornography, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256.
- b. Child erotica.
- c. Records and information relating to any computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
- d. Records and information relating to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C § 2256, or pertaining to an interest in child pornography, whether transmitted or received.
- e. Records and information concerning Kik or Meetme.



- f. Records, information, and communications concerning or discussing a sexual interest in Minors.
- g. Records and information relating to the ownership or possession of the PREMISES.
- h. Records and information relating to the email account [davebounts15@gmail.com](mailto:davebounts15@gmail.com), Kik account davebounts, and any other accounts used in furtherance of the Target Offenses.
- i. Records and information relating to online applications and cloud-storage applications that could be used to commit the Target Offenses, including usernames and passwords for those applications.
- j. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. evidence of the lack of such malicious software.
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation.
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence.
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.
- h. evidence of the times the COMPUTER was used.
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER.

- k. records of or information about Internet Protocol addresses used by the  
COMPUTER.
  - l. records of or information about the COMPUTER's Internet activity, including  
firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"  
web pages, search terms that the user entered into any Internet search engine, and  
records of user-typed web addresses.
  - m. contextual information necessary to understand the evidence described in this  
attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.